Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) In a cryptographic system wherein a certifying authority issues digital certificates identifying users of said system, said digital certificates being digitally signed with a private key of said certifying authority to form a digital signature and requiring a public key of said certifying authority in order to verify said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on information in said digital certificates and requiring said public key, a method of controlling access to said public key comprising ~~the steps of~~:

denying access to said public key;

providing said recipient with at least one message containing rules of said system, said rules including a rule regarding maintaining secrecy of said public key;

by said recipient, digitally signing said at least one message~~document~~, by which said recipient agrees to said rules; and

in response to said digital signing, permitting said recipient to utilize said public key.

2. – 17. (Canceled)

18. (New) The method of claim 1, wherein said providing includes providing said recipient with a secure device containing said public key, wherein said public key cannot be obtained from said secure device.

19. (New) The method of claim 1, wherein each user of the system has a private key, and wherein said rules include:

a rule requiring payment to a third party upon each use of said public key;

a rule requiring payment to a third party upon each use of a user's private key;

a rule requiring payment to a third party upon each certification of a certificate's status; or

a rule requiring payment to a third party upon each confirm-to transaction by a user.

20. (New) The method of claim 1, wherein said rules include a rule to pay for use by said recipient of intellectual property provided through the system.

21. (New) The method of claim 1, wherein said user transaction is invalid until said digital signing is performed.

22. (New) A method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising:

receiving, from a participant to a commercial transaction, a cryptographically authorized attribute approved by a sponsor;

checking the attribute presented to determine if the transaction may be processed and meet a requirement of the policy the attribute represents;

checking that the sponsor is valid in order that the transaction may be processed; and

determining to allow the transaction to be processed based upon the checking of the attribute and of the sponsor.

23. (New) The method of claim 22, further comprising determining to disallow the transaction to be processed if the checking of the attribute and of the sponsor is negative.

24. (New) The method of claim 22, further comprising agreeing to the policy and its encoding as an attribute.

25. (New) The method of claim 22, wherein the checking of the attribute and of the sponsor is automatic and comprising automatically processing the transaction.

26. (New) The method of claim 22, wherein the requirement of the policy defines:

an allowed document type of the transaction;

an allowed location at which the transaction may be formed;

an allowed time at which the transaction may be formed;

a time period within which a signature is valid;

a role which the participant may exercise;

a recipient of the transaction acceptable to the sponsor or to a certifying authority;
a sponsor of the participant that must be notified of and approve the transaction;
an entity that must be notified of the transaction; or
any combination of the foregoing.

27. (New) The method of claim 22, wherein the requirement of the policy defines:
a value limit for the transaction;
a co-signer requirement for the transaction; or
any combination of the foregoing.

28. (New) The method of claim 22, wherein the cryptographically authorized attribute comprises an attribute certificate signed by the sponsor, the participant's digital signature, information signed by a certification authority, information signed by a trusted third party, or any combination of the foregoing.

29. (New) The method of claim 22, further comprising receiving a digital identifying certificate issued by a certifying authority and having a field identifying the participant, wherein receiving the cryptographically authorized attribute comprises receiving a digital participant transaction including a digital message, a digital participant signature based on the digital message and on a private key of the participant and the attribute, and wherein the determining to allow the transaction comprises verifying the transaction based on information in the certificate and in the attribute.

30. (New) The method of claim 29, further comprising receiving a digital authorizing certificate, separate from the identifying certificate, issued by a sponsor of the participant and authorizing transactions by the participant, and wherein the determining to allow the transaction comprises verifying the transaction based on information in the authorizing certificate.

31. (New) The method of claim 30, wherein the digital authorizing certificate comprises the attribute to be applied to the digital message and wherein the determining to allow the transaction comprises applying the attribute to digital message to determine whether the transaction may be processed.

32. (New) The method of claim 22, further comprising processing content of the transaction, the attribute, or both using information contained in a portable microelectronic hardware device.

33. (New) The method of claim 32, wherein the information comprises a key and the portable microelectronic hardware device comprises a smart card.

34. (New) The method of claim 22, further comprising processing content of the transaction, the attribute, or both using biometric information of the participant.

35. (New) The method of claim 34, further comprising using the biometric information to access a smart card comprising information used to process the content of the transaction, the attribute, or both.

36. (New) The method of claim 22, further comprising processing content of the transaction based on a format of information defined in the policy and encoded as an attribute.

37. (New) The method of claim 22, wherein the policy defines systems rules, industry policy, industry-wide security policy and authorization information, pre-approved counter-party limitations, certification, restrictions on distribution of certificates, key confinement, document types and classes, signer roles and attributes, coded symbols, liability limitations, trust specifications, required attributes, allowable name forms, cross-certificates, binding information, trusted third parties, roles, identities, positive or negative restrictions pertaining to transaction subject matter, positive or negative restrictions pertaining to transaction context class, a confirm-to-requirement indication, a trusted time stamp, a time-stamp notary, information pertaining to the content of the transaction, information from third parties, electronic notarization, distribution restrictions, self-certification, an agreement for payment for the use of a commercial transaction system, price information, an agreement to pay for intellectual property, or any combination of the foregoing.

38. (New) The method of claim 22, wherein the cryptography comprises a digital signature of a sponsor, a digital signature of participant, a certificate signed by a sponsor, an attribute certificate, a certificate representing attributes, an individual signature, a digitally

signed electronic document, a message authentication code, a message encrypted using a symmetric key, a message encrypted using an asymmetric key, a message digest, a hash value, a signature and a message, a signature and an encrypted message, a public-key certificate, multiple signatures, a power-of-attorney certificate, a delegation certificate, a signature of a smart card, a hashed value within a signature of a message, or any combination of the foregoing.

39. (New) A method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising:

obtaining a cryptographically authorized attribute as approved by a sponsor, the attribute representing a requirement of the policy; and

presenting, by a participant to a commercial transaction, the cryptographically authorized attribute to a recipient, the recipient of the attribute to determine from the attribute if the transaction may be processed and meet the requirement and to check that the sponsor is valid in order that the transaction may be processed.

40. (New) The method of claim 39, comprising, prior to presenting the cryptographically authorized attribute, obtaining the cryptographically authorized attribute from the sponsor, a trusted third party or both.

41. (New) The method of claim 39, wherein the cryptographically authorized attribute comprises an attribute certificate signed by the sponsor, the participant's digital signature, information signed by a certification authority, information signed by a trusted third party, or any combination of the foregoing.

42. (New) The method of claim 39, comprising:

forming a digital message by the participant;

forming a digital participant signature based on the digital message and a private key of the participant;

combining the digital message and the digital participant signature to form a digital transaction; and

combining with the digital transaction a digital identifying certificate issued by a certifying authority, the identifying certificate having a field identifying the participant, and the attribute.

43. (New) The method of claim 42, further comprising combining with the digital transaction a digital authorizing certificate, separate from the identifying certificate, issued by the sponsor of the participant and authorizing transactions by the participant.

44. (New) The method of claim 43, wherein the digital authorizing certificate comprises the attribute to be applied to the digital message in order to determine whether the transaction may be processed.

45. (New) The method of claim 39, wherein the requirement of the policy defines:
an allowed document type of the transaction;
an allowed location at which the transaction may be formed;
an allowed time at which the transaction may be formed;
a time period within which a signature is valid;
a role which the participant may exercise;
a recipient of the transaction acceptable to the sponsor or to a certifying authority;
a sponsor of the participant that must be notified of and approve the transaction;
an entity that must be notified of the transaction; or
any combination of the foregoing.

46. (New) The method of claim 39, wherein the policy defines:
a value limit for the transaction;
a co-signer requirement for the transaction; or
any combination of the foregoing.

47. (New) The method of claim 39, further comprising processing content of the transaction, the attribute, or both using information contained in a portable microelectronic hardware device.

48. (New) The method of claim 47, wherein the information comprises a key and the portable microelectronic hardware device comprises a smart card.

49. (New) The method of claim 39, further comprising processing content of the transaction, the attribute, or both using biometric information of the participant.

50. (New) The method of claim 49, further comprising using the biometric information to access a smart card comprising information used to process the content of the transaction, the attribute, or both.

51. (New) The method of claim 39, further comprising presenting an attribute encoding a format of information, defined in the policy, based upon which the content of the transaction is to be processed.

52. (New) An electronic system for processing of commercial transactions according to a policy, comprising:

a first computer program code configured to receive, from a participant to a commercial transaction, transaction content and a cryptographically authorized attribute as approved by a sponsor;

a second computer program code configured to check the transaction content and the cryptographically authorized attribute to determine if the transaction may be processed and meet a requirement of the policy the attribute represents; and

a third computer program code configured to determine to allow the transaction to be processed based upon the check of the transaction content and the attribute.

53. (New) The system of claim 52, further comprising a fourth computer program code configured to facilitate agreement on the policy among a plurality of parties to an industry.

54. (New) The system of claim 52, further comprising a fifth computer program code configured to organize and recognize a participant within an organization and associate the participant with the sponsor.

55. (New) The system of claim 52, further comprising a sixth computer program code configured to obtain from the sponsor, a trusted third party, or both the cryptographically authorized attribute.

56. (New) The system of claim 52, further comprising a seventh computer program code configured to allow the sponsor, the trusted third party, or both to generate the cryptographically authorized attribute.

57. (New) The system of claim 52, further comprising an eighth computer program code configured to allow a participant to present the transaction content and the cryptographically authorized attribute to be checked to determine if the transaction may be processed and meet the requirement of the industry policy the attribute represents.

58. (New) The system of claim 52, further comprising a ninth computer program code configured to check that the sponsor is valid in order that the transaction may be processed.

59. (New) The system of claim 52, further comprising a tenth computer program code configured to automatically check the transaction content and the attribute and to automatically process the transaction.

60. (New) The system of claim 52, wherein the requirement of the policy defines:
an allowed document type of the transaction;
an allowed location at which the transaction may be formed;
an allowed time at which the transaction may be formed;
a time period within which a signature is valid;
a role which the participant may exercise;
a recipient of the transaction acceptable to the sponsor or to a certifying authority;
a sponsor of the participant that must be notified of and approve the transaction;
an entity that must be notified of the transaction; or
any combination of the foregoing.

61. (New) The system of claim 52, wherein the requirement of the policy defines:
a value limit for the transaction;
a co-signer requirement for the transaction; or
any combination of the foregoing.

62. (New) The system of claim 52, further comprising an eleventh computer program code configured to process content of the transaction, the attribute, or both using information contained in a portable microelectronic hardware device.

63. (New) The system of claim 62, wherein the information comprises a key and the portable microelectronic hardware device comprises a smart card.

64. (New) The system of claim 52, further comprising a twelfth computer program code configured to process content of the transaction, the attribute, or both using biometric information of the participant.

65. (New) The system of claim 64, further comprising a thirteenth computer program code configured to use the biometric information to access a smart card comprising information used to process the content of the transaction, the attribute, or both.

66. (New) The system of claim 52, further comprising a fourteenth computer program code configured to process content of the transaction based on a format of information defined in the policy and encoded as an attribute.

67. (New) The system of claim 52, further comprising a fifteenth computer program code configured to present an attribute encoding a format of information, defined in the policy, based upon which the content of the transaction is to be processed.

68. (New) A method for processing a commercial transaction employing cryptography to enforce a policy per transaction that is encoded at least in part as an attribute, comprising:

obtaining a cryptographically authorized attribute to be used by a participant to a commercial transaction, the attribute representing a requirement of the policy; and

approving by a sponsor the cryptographically authorized attribute, a recipient of the attribute from the participant to determine from the attribute if the transaction may be processed and meet the requirement and to check that the sponsor is valid in order that the transaction may be processed.

69. (New) The method of claim 68, wherein the cryptographically authorized attribute comprises an attribute certificate signed by the sponsor, the participant's digital signature, information signed by a certification authority, information signed by a trusted third party, or any combination of the foregoing.

70. (New) The method of claim 68, wherein the requirement of the policy defines:
an allowed document type of the transaction;
an allowed location at which the transaction may be formed;
an allowed time at which the transaction may be formed;
a time period within which a signature is valid;
a role which the participant may exercise;
a recipient of the transaction acceptable to the sponsor or to a certifying authority;
a sponsor of the participant that must be notified of and approve the transaction;
an entity that must be notified of the transaction; or
any combination of the foregoing.

71. (New) The method of claim 68, wherein the requirement of the policy defines:
a value limit for the transaction;
a co-signer requirement for the transaction; or
any combination of the foregoing.